APPLICATION

FOR

UNITED STATES PATENT

To all whom it may concern:

Be it known that we, Edwin O. Blew and Ker-Ming Chang, have invented certain new and useful improvements in:

Methods for Conducting Server-Side Encryption/Decryption-on-Demand

of which the following is a full and clear description:

METHODS FOR CONDUCTING SERVER-SIDE ENCRYPTION/DECRYPTION-ON-DEMAND

CLAIM OF PRIORITY

[0001] This application is a continuation-in-part of, claims priority to, and incorporates by reference in its entirety, co-pending U.S. patent application no. 09/343,921, filed on June 30, 1999.

FIELD OF THE INVENTION

[0002] The present invention is directed to methods and systems for securing files that are received, processed, stored, and delivered on or by typical web server applications, services, and devices.

BACKGROUND OF THE INVENTION

[0003] Many current web-based services receive and deliver encrypted files to and from external users or customers over electronic networks, such as the Internet. These web-based services often require their users to encrypt files prior to transmission and decrypt files upon receipt.

[0004] Requiring users of a service to encrypt and decrypt files typically requires time-consuming public key exchange procedures between the user and the service provider. In addition, it places a heavy burden on non-technical users who may not be familiar with dual-key encryption methods and tools. Furthermore, the encryption and decryption processes require the service provider to develop and establish a key management infrastructure that increases in complexity as the number of users using the service increases.

[0005] What is needed is a method and system for encrypting and decrypting electronic files that overcomes all of these concerns and problems while ensuring that strong protection and security are provided to important files.

SUMMARY OF THE INVENTION

[0006] The present invention implements a method used to secure computer files on a file server using dual-key encryption technologies without requiring the exchange of encryption keys with external users. The method may be embedded within one or more computer-readable programs, written in a programming language, such as Perl, and running on a web server. The method may employ the use of a single encryption/decryption key pair that is stored on the same web server to encrypt files received from external users on an inbound path and to decrypt files delivered to external users on an outbound path. All inbound and outbound encryption and decryption occurs in real time in a memory subsystem of the web server, which may include Random Access Memory (RAM). As a result, no unencrypted version of an electronic file needs to be created using the present invention. The method and system do not require any specific dual-key or public-private key encryption product or environment.

[0007] In a preferred embodiment of the present invention, a method of encrypting and decrypting an electronic file on a web-based computer system includes receiving, by a computer system, an electronic data file, where the computer system includes a memory subsystem and a plurality of memory locations, encrypting the data file in the memory subsystem, storing the encrypted data file in one or more of the plurality of memory locations, retrieving the encrypted data file from the one or more memory locations, decrypting the encrypted data file in the memory subsystem, and displaying the decrypted data file on a web browser. In an embodiment, the memory

subsystem includes random access memory. In an embodiment, the receiving step is performed using a SSL/HTTPS protocol. In an embodiment, the transmitting step is performed using a SSL/HTTPS protocol.

[0008] In an embodiment, the method may further include, prior to the receiving step, receiving a username and a password from an external user device and verifying that the username and password correspond to a pre-defined user having access to the computer system. In an alternate embodiment, the method further includes, between the storing step and the retrieving step retrieving the encrypted data file from the one or more memory locations, analyzing the encrypted data file, modifying the analyzed data file, and storing the modified data file in the one or more memory locations.

[0009] In an alternate embodiment, a method of encrypting and decrypting an electronic data file on a web-based computer system includes receiving, by a web server, an electronic data file, where the web server includes a memory subsystem, encrypting the data file in the memory subsystem, transmitting the encrypted data file to a file server having a plurality of memory locations, storing the encrypted data file in one or more of the plurality of memory locations, retrieving the encrypted data file from the one or more memory locations, transmitting the encrypted data file to the web server, decrypting the encrypted data file in the memory subsystem, and displaying the decrypted data file on a web browser. In an alternate embodiment, the method further includes, between the storing step and the retrieving step, retrieving the encrypted data file from the one or more memory locations, transmitting the encrypted data file to a back-end data processing server, analyzing, by the back-end data processing server, the encrypted data file, modifying, by the back-end data processing server, the analyzed data file, transmitting the modified data file to the file server, and storing the modified data file in the one or more memory locations.

[0010] In a preferred embodiment, a system for encrypting and decrypting an electronic data file includes a web server for encrypting a data file and decrypting an encrypted data file, the web server having a memory subsystem, a file server, electrically connected to the web server, for storing the encrypted data file, the file server having a plurality of memory locations, and a back-end data processing server, electrically connected to the file server, for modifying the encrypted data file. The web server includes a computer process for receiving the data file from an external user device, encrypting the data file in the memory subsystem, and transmitting the encrypted data file to a file server. The file server includes a computer process for receiving the encrypted data file from the web server, storing the encrypted data file in one or more of a plurality of memory locations, retrieving the encrypted data file from the one or more memory locations, and transmitting the encrypted data file to the back-end data processing server. The back-end data processing server includes a computer process for receiving the encrypted data file from the file server, analyzing the encrypted data file, modifying the analyzed data file, and transmitting the modified data file to the file server. In a further embodiment, the computer process of the file server further includes receiving the modified data file from the back-end data processing server, storing the modified data file in the one or more memory locations, retrieving the modified data file from the one or more memory locations, and transmitting the modified data file to the web server. In a further embodiment, the computer process of the web server further includes receiving the modified data file from the file server, decrypting the modified data file in the memory subsystem, and displaying the decrypted data file on a web browser.

[0011] In an alternate embodiment, a system for encrypting and decrypting an electronic data file includes a web server for encrypting a data file and decrypting an encrypted data file, the web server having a memory subsystem, and a file server electrically connected to the web server, for

storing the encrypted data file, the file server having a plurality of memory locations. The web server includes a computer process for receiving the data file from an external user device, encrypting the data file in the memory subsystem, and transmitting the encrypted data file to the file server. The file server includes a computer process for receiving the encrypted data file from the web server, storing the encrypted data file in one or more of the plurality of memory locations, retrieving the encrypted data file from the one or more memory locations, and transmitting the encrypted data file to the web server. In a further embodiment, the computer process of the web server further includes receiving the encrypted data file from the file server, decrypting the encrypted data file in the memory subsystem, and displaying the decrypted data file on a web browser. In an alternate embodiment, the computer process of the file server further includes, between the storing step and the retrieving step, retrieving the encrypted data file from the one or more memory locations, analyzing the encrypted data file, modifying the analyzed data file, and storing the modified data file in the one or more memory locations.

[0012] In an alternate embodiment, a system of for encrypting and decrypting an electronic data file includes a server including a memory subsystem, a plurality of memory locations, and a computer process for receiving a data file from an external user device, encrypting the data file in a memory subsystem, storing the encrypted data file in one or more of a plurality of memory locations, retrieving the encrypted data file from the one or more memory locations, decrypting the encrypted data file in the memory subsystem, and displaying the decrypted data file on a web browser. In a further embodiment, the computer process further includes, between the storing step and the retrieving step, retrieving the encrypted data file from the one or more memory locations, analyzing the encrypted data file, modifying the analyzed data file, and storing the modified data file in the one or more memory locations.

[0013] Further advantages and aspects of the present invention will become apparent to those of ordinary skill in the art upon reading and understanding the following detailed description of the invention.

BRIEF DESCRIPTION OF THE DRAWINGS

[0014] The invention may take form in various components and arrangements of components, and in various steps and arrangements of steps. The drawings are only for purposes of illustrating the preferred embodiments and are not to be construed as limiting the invention.

[0015] FIG. 1 depicts an exemplary diagram of the computer architecture and network connections used to implement an embodiment of the present invention.

[0016] FIG. 2 illustrates a data flow diagram of the inbound flow of files sent from an external user computer and the outbound flow of files to an external user computer according to an embodiment of the present invention.

[0017] FIG. 3 shows a program logic diagram for two computer program applications according to an embodiment of the present invention.

DETAILED DESCRIPTION OF THE INVENTION

[0018] Before the present methods and systems are described, it is to be understood that this invention is not limited to the particular methodologies, protocols, or systems described, as these may vary. It is also to be understood that the terminology used in the description is for the purpose of describing the particular versions or embodiments only, and is not intended to limit the scope of the present invention which will be limited only by the appended claims. In particular, although the present invention is described in conjunction with Internet files, it will be appreciated that the present invention may find use in any electronic exchange of data.

[0019] It must also be noted that as used herein and in the appended claims, the singular forms "a", "an", and "the" include plural reference unless the context clearly dictates otherwise. Thus, for example, reference to a "computer" is a reference to one or more computers and equivalents thereof known to those skilled in the art, and so forth. Unless defined otherwise, all technical and scientific terms used herein have the same meanings as commonly understood by one of ordinary skill in the art. Although any methods similar or equivalent to those described herein can be used in the practice or testing of embodiments of the present invention, the preferred methods are now described. All publications mentioned herein are incorporated by reference. Nothing herein is to be construed as an admission that the invention is not entitled to antedate such disclosure by virtue of prior invention.

[0020] FIG. 1 depicts an exemplary diagram of the computer architecture and network connections used to implement an embodiment of the present invention. A user computer **1** may be connected to a computer network **2**. The computer network **2** may include, without limitation, the Internet, an intranet, or any other interconnected network of computers. The connection of the user computer **1** to the computer network **2** may be achieved by any standard communication means including, but not limited to, a dialup service, a cable connection, a digital subscriber line, an Ethernet network interface, an Asynchronous Transfer Mode network interface, a wireless service, or similar technologies. A web server **3** running a standard http/https web server application may be used to transmit web pages to the user computer **1**. A file server **4** may store a plurality of incoming files until they are retrieved by a back-end data processing server **5**. In addition, the file server **4** may store outgoing files until they are retrieved by the user and sent to the user computer **1**. A back-end data processing server **5** may be used to host special purpose applications that may transform or modify encrypted files and generate outgoing user-deliverable files.

[0021] The computer/network architecture depicted in FIG. 1 is only one of many configurations that may be used to implement the method and system of the present invention. For example, the method or system may be implemented using only two servers, such as a web server and a combined file and back-end data processing server. Moreover, the method or system may be implemented entirely within a single server, such as a web server that performs all three functions described in reference to FIG. 1: web server, file server and back-end data processing server. However, the network architecture depicted in FIG. 1, and described in reference thereto, is preferred because it maximizes security by separating the data flow and processing across machines that may be separated by firewalls.

[0022] FIG. 2 illustrates a data flow diagram of the inbound flow of files sent from an external user computer and the outbound flow of files to an external user computer according to an embodiment of the present invention. The user computer **1** may access a login page **6** of a service provider's website using any web browsing application, such as Netscape Navigator or Microsoft's Internet Explorer. A user may supply an assigned username and password when accessing the login page **6** in order to access the web server **3**. The transmission of the login page **6** and all subsequently described pages and files transmitted between the user computer **1** and the web server **3** may utilize the secure SSL/HTTPS protocol standard. The login page **6** of the preferred embodiment may be used to provide an additional layer of security. However, the login page **6** may be removed where user authentication via the submission of a username and/or a password is unnecessary, but encryption/decryption-on-demand is still required.

[0023] A user may select a file stored locally on the user computer **1** and submit the file for processing by the web server **3** via a file upload web page **7**. The file upload process may be achieved through use of a standard HTML tag, such as <form><input type="file"

name="filename"></form>. The upload transmission may be securely transmitted via use of the SSL/HTTPS protocol standard, which provides an additional layer of security to the transmission environment. In an alternate embodiment, the SSL/HTTPS standard is not used for the transmission of one or more of the transmitted files between the user computer **1** and the web server **3**.

[0024] A computer program **8** written in a computer-recognizable language, such as Perl, and stored on the web server **3**, may be used to process an incoming electronic data file. The process of encrypting the program is depicted in FIG. 3. The electronic data file may be processed by reading the data file in unencrypted form **16** from a buffer on the web server **3** into a memory subsystem of the web server. The memory subsystem may include one or more memory devices, including, without limitation, Random Access Memory (RAM). The content of the data file may then be encrypted **17** in the memory subsystem via a system call to an encryption application, such as PGP. The encrypted data content may be saved **18** to a file on the web server **3**. The encrypted data file may then be transferred **9** from the web server **3** to the file server **4**. This transfer may be performed via a File Transfer Protocol (FTP) program or any similar program for transferring files between servers.

[0025] In an alternate embodiment, a computer application environment other than Perl may be used to implement the present invention. In fact, any application environment permitting direct system calls (e.g., to an encryption utility) and Common Gateway Interface (CGI) interactions with a web server may be used. Moreover, the present invention may be implemented via the use of dual-key encryption technologies other than PGP or through the use of single-key or other encryption methodologies.

[0026] Once the encrypted data file is stored on the file server **4**, additional processing of the encrypted data file on the back-end data processing server **5** may be performed. Such additional

processing is optional to the present invention. The additional processing may include using a FTP program to send **10** the encrypted data file from the file server **4** to the back-end data processing server **5**. The encrypted data file may then be analyzed, modified and/or rewritten **11** by the back-end data processing server **5**, and transferred back **12** to the file server **4** as an encrypted user-deliverable data file.

[0027] When requested by a user, the encrypted user-deliverable data file may be transferred **13** from the file server **4** to the web server **3** by using a FTP program. A computer program **14** written in a computer-recognizable language, such as Perl, and stored on the web server **3**, may be used to decrypt the outgoing encrypted user-deliverable data file. The process of decrypting the file is depicted in FIG. 3. The encrypted user-deliverable data file may be read in encrypted form **19** from a buffer on the web server **3** into the memory subsystem. The file content may be decrypted in the memory subsystem via a system call to a decryption application, such as PGP, and the encrypted data file may be deleted from the system **20**. The decrypted content in the memory subsystem may then be downloaded **21** to the user's browser **15** via a buffer on the web server **3**.

[0028] The two computer programs **8**, **14** may perform additional functions that are not essential to the implementation of the present invention. The additional, non-essential functions are part of the preferred embodiment of the present invention, however, and are referenced herein to show the implementation of the preferred embodiment. The additional, non-essential functions in computer program **8** may include, without limitation, the user authentication process including the reception of a username and password. The additional, non-essential functions in computer program **14** may include, without limitation, a means for creating a web page (dynamically) listing all available user-deliverable files and allowing the user to choose which file to decrypt and download.

[0029] The foregoing is considered as illustrative only of the principles of the invention. Further, since numerous modifications and changes will readily occur to those skilled in the art, it is not desired to limit the invention to the exact construction and operation shown and described, and accordingly, all suitable modifications and equivalents may be resorted to, falling within the scope of the invention.